Management's Response	Following are management responses to each of the above observations: a) Management concurs with the finding. Although all of the DASD is mirrored an all DASD that are non-transient are backed up to tape, a formal policy will be developed. b) Management concurs with the finding that UDC and DOES backup tapes were not being sent offsite with the DHS and DMV tapes. The issue was resolved by including the UDC and DOES backup under the contract with First Federal (PO133695).

Process	Information Technology General Controls at the ODC1 and ODC2 Data Centers
Title	Service Level Agreements
Observation	Management has not established service level agreements (SLA) for ODC-1 and ODC-2 data center users. Management has begun the process of identifying SLA standards for users of both data centers. However, these standards have not been formalized nor documented to date. Without defined and written service level agreements, there may be a misunderstanding about the level of services to be provided. For example UDC expected ODC-1 to backup its data, while ODC-1 expected UDC to backup its own data. As a result UDC data was not backed-up.
Recommendation	We recommend that management establish and implement service level agreements with ODC-1 and ODC-2 users. Before establishing SLA, OCTO should develop standards for providing services and metrics for evaluating the services provided. Through the SLA, system users and the information services function should have a written agreement that describes the service level in qualitative and quantitative terms. This agreement should define the responsibilities of both OCTO and the Agency.
Management's Response	Management concurs with the findings. As Executive Management has changes, so have perspectives on Service Level Agreements. The current Executive Management Team is committed to the establishment of Operating Level Agreements. (For a proper SLA, one must have end-to-end control over all of the components of the service. An OLA would only cover the components over which control is exercised.)

Process	Information Technology General Controls
Title	Disaster Recovery and Backup Strategy
Observation	Each District agency is currently responsible for developing its own disaster recovery and business continuity plan. Disaster recovery processes at the District are not integrated across all critical agencies of the District of Columbia to ensure that no single point of failure could have a disastrous effect on critical business functions. A District-wide view of what needs to be done to continue operations, in case of an interruption of IT services, is not in place at the District. Additionally, we observed the following regarding the Office of Chief Technology Officer (OCTO): (1) OCTO's disaster recovery plans are not finalized and have not been tested. A business impact analysis has not been performed at the two data centers (ODC1 and ODC2) to A) determine the impact of interruptions to specific processes and the overall operation of each data center B) to incorporate the operations and functional aspects of an interruption. (2) The current disaster recovery strategy for the two OCTO data centers is mutual backup. OCTO is working towards having each data center provide disaster recovery for the other. The disaster recovery facilities are partially in place with the installation of the Enterprise Tape System (ETS), which will mirror ODC2 data at ODC1. Real time mirroring of ODC1 data at ODC2 is yet to be implemented. If the ODC1 data center was to be out of service for an extended period of time, the ODC2 data center is not prepared to provide a disaster recovery capability. This mutual backup strategy is sound in every respect, except for the fact that the two data centers are less than four miles apart. We are concerned that both data centers could be vulnerable to a single event, or to a coordinated attack specifically directed to both data centers. OCTO does not have a fall-back plan or capability to recover data center operations at a secure disaster recovery site outside the Washington metropolitan area.
Recommendation	OCTO should develop a comprehensive enterprise-wide business continuity plan (BCP) that addresses all agencies maintaining mission critical financial application systems as well as the data centers. The enterprise-wide BCP can incorporate/reference the BCPs developed by OCTO and each agency. Agencies with missing or out-dated BCPs, if any, should develop and test a BCP and submit it to OCTO for inclusion in the enterprise-wide BCP. OCTO can then determine the cohesiveness and feasibility of the enterprise-wide BCP.

Process	Information Technology General Controls
Title	Disaster Recovery and Backup Strategy
Observation	Each District agency is currently responsible for developing its own disaster recovery and business continuity plan. Disaster recovery processes at the District are not integrated across all critical agencies of the District of Columbia to ensure that no single point of failure could have a disastrous effect on critical business functions. A District-wide view of what needs to be done to continue operations, in case of an interruption of IT services, is not in place at the District. Additionally, we observed the following regarding the Office of Chief Technology Officer (OCTO): (1) OCTO's disaster recovery plans are not finalized and have not been tested. A business impact analysis has not been performed at the two data centers (ODC1 and ODC2) to A) determine the impact of interruptions to specific processes and the overall operation of each data center B) to incorporate the operations and functional aspects of an interruption. (2) The current disaster recovery strategy for the two OCTO data centers is mutual backup. OCTO is working towards having each data center provide disaster recovery for the other. The disaster recovery facilities are partially in place with the installation of the Enterprise Tape System (ETS), which will mirror ODC2 data at ODC1. Real time mirroring of ODC1 data at ODC2 is yet to be implemented. If the ODC1 data center was to be out of service for an extended period of time, the ODC2 data center is not prepared to provide a disaster recovery capability. This mutual backup strategy is sound in every respect, except for the fact that the two data centers are less than four miles apart. We are concerned that both data centers could be vulnerable to a single event, or to a coordinated attack specifically directed to both data centers. OCTO does not have a fall-back plan or capability to recover data center operations at a secure disaster recovery site outside the Washington metropolitan area.
Recommendation	OCTO should develop a comprehensive enterprise-wide business continuity plan (BCP) that addresses all agencies maintaining mission critical financial application systems as well as the data centers. The enterprise-wide BCP can incorporate/reference the BCPs developed by OCTO and each agency. Agencies with missing or out-dated BCPs, if any, should develop and test a BCP and submit it to OCTO for inclusion in the enterprise-wide BCP. OCTO can then determine the cohesiveness and feasibility of the enterprise-wide BCP.

	The BCP for OCTO should include not only the Disaster Recovery measures but also the operations and functional measures required for full recovery of all business functions at OCTO, as well as the IT functions. OCTO business continuity plans should be updated, reviewed, and tested on a regular basis to ensure consistency of business operations. Further, OCTO should secure an agreement with a commercial disaster recovery site outside the immediate metropolitan Washington area to ensure adequate backup facilities exist in the event of a major attack on the District that interrupts operations at both data centers. Finally, OCTO should complete implementation of real-time mirroring of ODC1 data at the ODC2 data center to ensure more timely recovery of data in case of a disaster.
Management's Response	Management concurs with the overall finding. Management concurs that the DR plans are neither finalized (fully documented) nor fully tested. (Although the District has successfully performed an internal test using a clone of the DMV LPAR, a full-function test of the DR process still needs to be performed.) Management also concurs that the mirroring between ODC1 and ODC2 needs to be completed. (The District is currently mirroring all of the DASD and the ODC2 Tapes. Completion of the mirroring of the ODC1 tapes remains to be completed.) Management agrees that if prior to completion of the mirroring of the tapes, ODC1 had to be serviced through ODC2 then it would be more laborious and time consuming than if ODC2 had to be serviced through ODC1.

Process	Information Technology General Controls
Title	IT Governance Program
Observation	A comprehensive governance program for high cost, high exposure, and mission critical IT projects at the District is not in place.
Recommendation	We recommend that a single *Project Management Office* (PMO) be established as the operational arm of the Architecture Committee of a comprehensive IT Governance Program. The PMO's role would be to gather information needed for decision-making, provide the detail coordination necessary for implementation of Committee initiatives, and monitor and report progress. Components of a strong IT governance program include: a. An *IT Steering Committee* is comprised of senior executives and business unit executives. The role of the steering committee is to identify key business